IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	§	Group Art Unit: 2143
	§	Examiner: Bilgrami, Asghar H.
Thomas E. Tahan	§	Atty. Dkt. No.: 5181-75800/P5413
	§	
	§	
	§	****CERTIFICATE OF E-FILING TRANSMISSION****
Serial No. 09/981,608	§	I hereby certify that this correspondence is being transmitted via electronic filing to the United States Patent and Trademark Office on the date shown below
	§	
	§	Rory D. Rankin
Filed: October 16, 2001	§	Printed Name
	§	
For: COMMUNITY ACCESS CONTROL IN A MULTI-COMMUNITY NODE	§	/ Rory D. Rankin / (Signature) April 18, 2008 (Date)
	§	
	§	
	§	
	§	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Further to the Notice dated February 19, 2008, Appellants present this Appeal Brief. Appellants respectfully request that this appeal be considered by the Board of Patent Appeals and Interferences.

I. REAL PARTY IN INTEREST

As evidenced by the assignment recorded at Reel/Frame 012274/0312, the subject application is owned by Sun Microsystems, Inc., a corporation organized and existing under and by virtue of the laws of the State of Delaware, and now having its principal place of business at 4150 Network Circle, Santa Clara, CA 95054.

II. RELATED APPEALS AND INTERFERENCES

No other appeals, interferences or judicial proceedings are known which would be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-6, 9-15, 17-23, 25-31 and 34 are pending and rejected, and are the subject of this appeal. A copy of claims 1-6, 9-15, 17-23, 25-31 and 34 as on appeal is included in the Claims Appendix hereto.

IV. STATUS OF AMENDMEMNTS

No amendments to the claims have been submitted subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The subject matter of the present claims generally relates to the field of computer network security in multi-community computing nodes.

Claim 1 recites a method of community access control in a Multi-Community Node (MCN). In an enterprise network, some computing resources may be dedicated to users of a single community, and others may be shared among users of multiple communities. A Multi-Community Node (MCN) is a network node which processes information on behalf of individuals in more than one community. (e.g., *see 1010 of Figure 10; pp. 29-30; pp. 1-2*). In contrast, Single Community Nodes (SCNs) are network nodes (e.g., computers, networking equipment, etc.) processing information on behalf of users in a single community. Examples of MCNs include servers and routers. Executing on MCNs are Multi-Community Applications (MCAs). MCAs are software applications performing functions on behalf of users in more than one community. (e.g., *see 1020 of Fig. 10).*

The method of claim 1 comprises receiving a request for access to an object. Objects may include file systems, storage volumes, directories, files, memory regions, queues, pipes, sockets, input/output devices, or other operating system controlled resources. (*e.g., p. 25, lines 17-19*).

The method further comprises consulting a community information base (CIB) responsive to said request, wherein said CIB includes: a user community set (UCS) for each user of said MCN, wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community; an application community set (ACS) for each application on said MCN, wherein for a given application and associated ACS, a given community is a member of the ACS if the given application runs on behalf of a user in the given community; and an object community set

(OCS) for each object residing within said MCN, wherein each OCS is included in an ACS of a process which created it (*e.g., see 1060 of Fig. 10; p. 25, lines 4-8; page 9, lines 20-24; page 25, lines 4-16*).

The method further comprises permitting access to said object in response to detecting: said request is from a user; and a UCS of said user is a superset of an OCS of said object; denying access to said object in response to detecting said request is from the first user; and a UCS of the first user is not a superset of an OCS of said object;. (*e.g., page. 4, lines 22-25*).

The method further comprises permitting access to said object in response to detecting: said request is from a process; and an ACS of said process is a superset of an OCS of said object; and denying access to said object in response to detecting said request is from said process; and an ACS of said process is not a superset of an OCS of said object. (*e.g., page 26, lines 11-16*); wherein a given OCS comprises a first set of communities, a given UCS is a superset of the given OCS if at least all of the first set of communities are also included in the given UCS, and a given ACS is a superset of the given OCS if at least all of the first set of communities are also included in the given ACS.

Claim 10 recites a Multi-Community Node (MCN). As discussed above, a Multi-Community Node is a network node which processes information on behalf of individuals in more than one community. (e.g., s*ee 1010 of Figure 10; pp. 29-30; pp. 1-2*). Claim 10 recites the MCN comprises a community information base (CIB) which includes a user community set (UCS) for each user of said MCN, wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community; an application community set (ACS) for each application on said MCN, wherein for a given application and associated ACS, a given community is a member of the ACS if the given application runs on behalf of a user in the given community; and an object community set (OCS) for each object residing within said

MCN, wherein each OCS is included in an ACS of a process which created it (*e.g., see 1060 of Fig. 10; p. 25, lines 4-8; page 9, lines 20-24; page 25, lines 4-16*). In addition, the MCN is recited as including a processing unit which is configured to receive a request for access to an object (*e.g., p. 25, lines 17-19*), and consult the CIB responsive to said request. The processing unit is further configured to permit access to said object in response to detecting said request is from a user; and a UCS of said user is a superset of an object community set (OCS) of said object (*e.g., page. 4, lines 22-25*). The processing unit is configured to deny access to said object in response to detecting said request is from the first user; and a UCS of the first user is not a superset of an OCS of said object. The processing unit is also configured to permit access to said object in response to detecting said request is from a process; and an ACS of said process is a superset of said OCS. The processing unit is configured to deny access to said object in response to detecting said request is from said process; and an ACS of said process is not a superset of an OCS of said object; (*e.g., page 26, lines 11-16).*

Claim 18 recites a computer system comprising a computer network and a multi-community node (MCN). See the discussion above regarding claim 10 for a summary regarding the recited MCN.

Claim 26 recites a carrier medium comprising program instructions. The program instructions are generally executable to perform the method recited in claim 1. See the discussion above regarding claim 1 for a summary regarding the recited features.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-6, 9-15, 17-23, 25-31 and 34 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,265,221 (hereinafter "Miller") in view of U.S. patent 6,772,350 (hereinafter "Belani").

VII. ARGUMENT

1. Claims 1-6, 9-15, 17-23, 25-31 and 34 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,265,221 (hereinafter "Miller") in view of U.S. patent 6,772,350 (hereinafter "Belani"). Appellants traverse these rejections for the following reasons.

Claims 1, 10, 18 and 26

Miller and Belani do not disclose, teach, or suggest, either separately or in combination, at least the recited CIB which includes "an application community set (ACS) for each application on said MCN" as recited in claim 1. In rejecting claim 1, the Examiner states in paragraph 5 of the Office Action dated October 18, 2007:

> "As per claims 1, 10, 18 & 26 Miller disclosed a computer system comprises: a Multi-community Node (MCN) comprises: a community information base (CIB), wherein said (CIB) (col. 2, lines 42-47) includes: a user community ser (UCS) for each user of said MCN, wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community (col. 4, lines 57-67 & col. 5, lines 1-20); an application community set (ACS) for each application on said MCN, wherein for a given application and associated ACS, a given community is a member of the ACS if the given application runs on behalf of a user in the given community (col. 5, lines 22-62); and an object set (OCS) (col. 1, lines 30-35) for each object residing within said MCN (col. 2, lines 52-62), wherein each OCS is included in an ACS of a process which created it . . . said request is from a process; and an ACS said process is a superset of said OCS (col. 5, lines 39-62). . . .
>
> However Miller did not explicitly disclose a computer network coupled to the Multi-community node (MCN). In the same field of endeavor Belani disclosed a computer network; and a multi-community node (MCN) coupled to said computer network (col. 4, lines 34-38). At the time the invention was made it would have been obvious to one in the ordinary

> skill in the art to incorporate a connection to computer network as disclosed by Belani to a computer system of Miller in order to make the computer system more versatile and scalable by having multiple clients/users connect to the system from various locations."

By way of preface, a community set is defined on page 9 of the Description as follows: "A "Community Set" is a set of communities, which may consist of no communities (the null community set) or any number of communities. Each individual community within the community set is said to be a "member" of the set." As seen from the above rejection, the Examiner states that Miller disclosed a CIB which includes "an application community set (ACS) for each application on said MCN." Appellant respectfully disagrees. In contrast, Miller merely discloses access control mechanisms based on stored user attributes. More specifically, Miller discloses:

> "A still further object of the invention is to provide an access control mechanism . . . using customer-supplied attributes of users and objects, as well as customer-defined verbs.
>
> According to the present invention, as embodied and broadly described herein, an access control mechanism using a processor is provided for specifying access control policies to entities, comprising subject means, verb means, object means, definition means, rule means and evaluation means. The processor may be embodied as a microprocessor and memory, or computer using software. The subject means stores user information in a matrix having information for each user on each row, and user attributes pertaining to the specific user in each field (column)." (Miller, col. 2, lines 32-52).

As may be seen from the above, Miller describes storing user attributes in a matrix. However, Miller's disclosures are not equivalent to the recited UCS "wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community," as is recited in claim 1. The apparatus of Miller is a rather complex collection comprising a subject means, verb means, object

means, definition means, rule means and evaluation means. However, Appellant submits nothing in the above disclosure teaches or suggests a CIB including the "application community set (ACS) for each application on said MCN" as recited. Further, Applicant submits a table of user attributes as disclosed in Miller is clearly not equivalent to a user community set (UCS) - or a community set at all as described and defined in the presently claimed invention. Nor are the disclosures of Miller equivalent to an application community set or object community set, as recited. For at least these reasons, Applicant submits claim 1 is patentably distinct from the cited art. Likewise, as each of dependent claims 2-6, 9, 11-15, 17, 19-23, 25, 27-31, and 34 includes at least the features of the above independent claims upon which it depends, each of dependent claims 2-6, 9, 11-15, 17, 19-23, 25, 27-31, and 34 is believed patentable as well.

The Examiner further suggests that a "processing unit configured to … permit access to said object in response to detecting said request is from a user; and a UCS of said user is a superset of an object community set (OCS) of said object," is disclosed by Miller at col. 4, lines 56-col. 5, line 20. However, the cited portion of Miller merely describes group security policies. More particularly, Miller discloses:

> "Security policies are concerned not only with which subject may obtain access to which objects, but also with the granting, revoking, and denying of authorizations to and from users and groups. Given the set of authorizations for users and groups, some rule must be applied for deriving authorization for subjects.
>
> In the general case, a user may belong to more than one group. In assigning privileges to subjects acting on behalf of a user, one can choose to:
>
> 1. Have the subject operate with the union of privileges of all the groups to which the user belongs, as well as all his or her individual privileges;
> 2. Have the subject operate with the privilege of only one group at a time;
> 3. Allow the subject to choose whether to operate with its user's privileges or with the privileges of one of the groups to which its user belongs; and
> 4. Implement some other policy.

> Note that even if a subject S is constrained to be associated with at most one group to which its associated user belongs, a user is still not constrained to operate with the authorizations of only one group at a time. For example, if user U belongs to a group G1 that is authorized for a relation or view R and U also belongs to another group G2 that has been specifically denied authorization for R, then U can still gain access to R by employing a subject whose associated group is G1, unless U has also been individually denied authorization for R. Thus, this choice of policy constrains subjects rather than users, and can be thought of as a form of least privilege." (Miller, col. 4, line 57 - col. 5, line 20).

As may be seen from the above, Miller bases security policies on privileges of users and/or on combinations of privileges of the groups to which users belong. However, as argued above, Miller does not disclose maintaining a UCS or an OCS in a CIB. The attributes Miller stored are privileges, not community sets. Therefore, not only does Miller not disclose basing authorization on whether or not a UCS is a superset of an OCS, but it would not have been obvious to one of ordinary skill in the art at the time of the invention to base authorization on such a criterion, since the information needed to determine the necessary condition, a UCS and an OCS, is not stored in Miller's matrix. Instead Miller suggests that the privileges of users and groups are what is maintained and access authorization is determined by combining privileges of users and groups according to some set of rules. Accordingly, Applicant finds no teaching or suggestion in the cited art of "detecting said request is from a user; and a UCS of said user is a superset of an object community set (OCS) of said object," as is recited in claim 1. Moreover, since Miller's matrix does not include the concept of a community set, claim limitations directed toward an object community set or an application community set are also distinguished from the cited art.

In addition to the above, the Examiner further states that Miller disclosed a processing unit configured to "permit access to said object in response to detecting: said

request is from a process; and an ACS [of] said process is a superset of said OCS (col. 5, lines 39-62)." Appellant respectfully disagrees. Again, for convenience, the portion of Miller cited by the Examiner is reproduced below:

> " Ownership
>
> It is probably an application-dependent choice whether an object can have more than one owner. Ownership policies are sometimes implemented so that only the owner of an object has the right to delete or modify the object. However, in many commercial database systems, multiple users can have such authorizations for the same relation or view. Ownership could alternatively be interpreted as the right to grant and revoke authorizations for an object to and from other users. However, in any system that uses copyflags (such as Oracle) or that has access modes for grant and/or give-grant (as does SeaView [4, 5]), many users could have such authorizations. Although a special user, such as database administrator or security officer, may be able to grant and revoke authorizations that were not explicitly granted to him or her, that special user should not be able to revoke authorizations from the owner (although this may also be an application-dependent choice). A facility that allows an appropriate ownership policy for the organization to be defined at system installation would allow vendors to provide the comprehensiveness and flexibility of control to cover most applications, access control requirements while avoiding having to "wire in" a fixed ownership policy." (Miller, col. 5, lines 38-62).

However, this disclosure of Miller merely provides a general discussion concerning ownership and nothing in this disclosure teaches a processing unit configured to "permit access to said object in response to detecting: said request is from a process; and an ACS of said process is a superset of said OCS of said object." Further, neither does this disclosure of Miller disclose the "application community set (ACS) for each application on said MCN" as recited.

In addition to the above, upon review of the remainder of Miller (those portions not cited by the examiner), not only is it apparent that the above discussed features are not

disclosed, but the nature of the mechanism disclosed by Miller is quite different from that presently claimed.

For example, Miller discloses storing information about subjects, objects, verbs, rules, and definitions. In particular, Miller discloses:

> "In the embodiment shown in FIG. 2, the subject memory 204 stores user information in a logical matrix having a specific user on each row, with user attributes, i.e. data pertaining to the specific user, in each field (column). The object memory 206 stores object names and object attributes and optionally object rules for defined verbs. The verb memory 208 stores verb names with a default rule for each verb name. The rule memory 210 stores rule names with their associated boolean expressions. The definition memory 212 stores field definitions, external function declarations, and strings. The evaluator 202, coupled to the subject memory 204, object memory 206, verb memory 208, the rule memory 210 and the definition memory 212, allows or disallows access of the user 102 to the entity 106 according to the specified verb, specified default rule, and user and object attributes." (Miller, col. 4, lines 14-30, emphasis added).

This verb, rule, attribute mechanism taught by Miller is quite distinct from the presently recited features of claim 1. Further, in Fig. 5 and related text, Miller describes an object window which includes object names and corresponding rules for defined verbs. For example, Miller teaches:

> "The object window, shown in FIG. 5, is used to display and update object names and rules for defined verbs. The information displayed in the object window corresponds to the data stored in the object memory 206. In FIG. 5, information preceding the colon (:) is either the name of the object or an attribute of the object, the semantics being defined via the definition window. Everything after the object name is considered to be a rule list. Rules for specific verbs are designated as:
>
> <verb name>: <rule>
>
> Object rules must be separated by semicolons (;).

> In this window, rule names, defined in the rule window, are prefixed by a colon (:) and verb names, defined in the verb window, are suffixed by a colon (:). For example, one of the rules specified above for object "$VXYZ FILE_2" is:
>
> W: :MEMBER_OF_A & SUBJ.NAME <>'NABER';
>
> The verb W (WRITE) is defined in the verb window, and the rule $MEMBER_{13}$ OF_{13} A is defined in the rule window. This means that the verb W can be invoked for object $VXYZ $FILE_{13}$ 2 only if the rule $MEMBER_{13}$ OF_{13} A satisfied. The other part of the rule, "& SUBJ.NAME <>`NABER`", means that even if the rule $MEMBER_{13}$ OF_{13} A is satisfied, write access by NABER is specifically denied. The write rule for object "$VXYZ $FILE_{13}$ 1" indicates that the user must be on the access control list ACL_{13} 1, as specified in in [*sic*] the definition window." (miller, col. 8, line 63 – col. 9, line 26).

In the above, it can be seen that Miller discloses access control to an object by providing a <object name> : <verb_name> :: <rule> combination. In the example, it is determined whether a user may write to a file $VXYZ FILE_2. If the user is a member of A (and is not NABER), then the user may write to the file. Clearly, such a teaching is not equivalent to that as recited wherein "an ACS of said process is a superset of an OCS of said object." Note there is no teaching of an OCS of said object. Neither is there a teaching of an ACS of said process being a superset of the OCS. Further, the teaching describes determining if a user is a member of A (e.g., is the user a member of a group A). Apart from the other distinctions, even this teaching at best would merely ask whether the user is a member of a group. Again, such an approach is not equivalent to "an ACS of said process is a superset of an OCS of said object."

Appellant submits the above teaching of Miller further makes clear that Miller discloses a fundamentally different method and mechanism than that recited by the

Appellant. In view of the above discussion, as the cited references do not teach or suggest all of the features of claim 1, either singly or in combination, Appellants submit the Examiner has not established a prima facie case of obviousness. For at least the reasons provided above, the rejection of claim 1 is not supported by the cited art. Withdrawal of the rejection to claim 1, and claims dependent thereon, is respectfully requested.

Appellant further notes each of independent claims 10, 18 and 26 include features similar to those discussed above and are patentably distinguishable for similar reasons. Accordingly, withdrawal of the rejections of claims 10, 18 and 26, and claims dependent thereon, are respectfully requested.

Claims 5, 14, 22 & 30

Claim 5 recites the features "further comprising permitting an owner of said object to designate a first user as a new owner of said object, in response to detecting a UCS of said first user is a superset of said OCS." Appellant submits these features are neither taught nor suggested in the cited art.

In the Office Action dated October 18, 2007 (paragraph 9), the Examiner states that the above features are taught by Miller at column 5, lines 39-62 (already discussed above). However, this disclosure of Miller merely provides a general discussion regarding ownership. It is first noted that the cited disclosure nowhere teaches "permitting an owner of said object to designate a first user as a new owner of said object." At best, the cited disclosure states "Ownership could alternatively be interpreted as the right to grant and revoke authorizations for an object to and from other users" which is not equivalent. Further, the features recite that the permission is "in response to detecting a UCS of said first user is a superset of said OCS." Nothing in the cited disclosure teaches such features. As already discussed above, these set, and set operations as recited are not disclosed. In

view of the above discussion, as the cited references do not teach or suggest all of the features of claim 5, either singly or in combination, Appellants submit the Examiner has not established a prima facie case of obviousness. For at least the reasons provided above, the rejection of claim 5 is not supported by the cited art. Withdrawal of the rejection to claim 5 is respectfully requested.

Appellant further notes each of dependent claims 14, 22 and 30 include features similar to those of claim 5 and are patentably distinguishable for similar reasons. Accordingly, withdrawal of the rejections of claims 14, 22 and 30 is respectfully requested.

Claims 6, 15, 23 & 31

Claim 6 recites the additional features "further comprising allowing a first process to change said OCS of said object to a subset of said ACS of said first process, in response to detecting an owner of said first process is an owner of said object and said ACS is a superset of said OCS." Appellant submits these features are neither taught nor suggested in the cited art.

In Office Action, the Examiner states that the above features are taught by Miller at column 5, lines 39-62 (already discussed above). However, this disclosure of Miller merely provides a general discussion regarding ownership. Nothing in this disclosure includes "allowing a first process to change said OCS of said object to a subset of said ACS of said first process." In contrast, the cited disclosure merely states "[a]lthough a special user, such as database administrator or security officer, may be able to grant and revoke authorizations that were not explicitly granted to him or her, that special user should not be able to revoke authorizations from the owner." Appellant submits this disclosure is not equivalent to "allowing a first process to change said OCS of said object

to a subset of said ACS of said first process." Further, it is noted that claim 6 recites said allowing is "in response to detecting an owner of said first process is an owner of said object and said ACS is a superset of said OCS." Such features are not disclosed in the cited teaching of Miller and are nowhere disclosed in Miller as suggested.

In view of the above discussion, as the cited references do not teach or suggest all of the features of claim 6, either singly or in combination, Appellants submit the Examiner has not established a prima facie case of obviousness. For at least the reasons provided above, the rejection of claim 6 is not supported by the cited art. Withdrawal of the rejection to claim 6 is respectfully requested.

Appellant further notes each of dependent claims 15, 23 and 31 include features similar to those of claim 6 and are patentably distinguishable for similar reasons. Accordingly, withdrawal of the rejections of claims 15, 23 and 31 is respectfully requested.

Claims 9, 17, 25 & 34

Claim 9 recites the further features "wherein said CIB further includes a creator and a current owner for each object residing within said MCN." Appellant submits these features are neither taught nor suggested in the cited art.

In the Office Action, the Examiner states that the above features are taught by Miller at column 5, lines 39-62 (already discussed above). However, this disclosure of Miller merely provides a general discussion regarding ownership. Nothing in this disclosure includes "wherein said CIB further includes a creator and a current owner for each object residing within said MCN." Further, nothing in this disclosure mentions the creator of an object.

In view of the above discussion, as the cited references do not teach or suggest all of the features of claim 9, either singly or in combination, Appellants submit the Examiner has not established a prima facie case of obviousness. For at least the reasons provided above, the rejection of claim 9 is not supported by the cited art. Withdrawal of the rejection to claim 9 is respectfully requested.

Appellant further notes each of dependent claims 17, 25 and 34 include features similar to those of claim 6 and are patentably distinguishable for similar reasons. Accordingly, withdrawal of the rejections of claims 17, 25 and 34 is respectfully requested.

Conclusion

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-6, 9-15, 17-23, 25-31 and 34 was erroneous, and reversal of his decision is respectfully requested.

No fees are believed necessary; however, the Commissioner is hereby authorized to charge any fees which may be required to Deposit Account No. 501505/5181-75800/RDR.

Respectfully submitted,

/Rory D. Rankin/

Rory D. Rankin
Reg. No. 47,884
Attorney for Appellants

Meyertons, Hood, Kivlin,
Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
(512) 853-8850

Date: April 18, 2008

VIII. CLAIMS APPENDIX

The claims on appeal are as follows.

1. A method of community access control in a Multi-Community Node (MCN), said method comprising:

receiving a request for access to an object;

consulting a community information base (CIB) responsive to said request, wherein said CIB includes:

a user community set (UCS) for each user of said MCN, wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community;

an application community set (ACS) for each application on said MCN, wherein for a given application and associated ACS, a given community is a member of the ACS if the given application runs on behalf of a user in the given community; and

an object community set (OCS) for each object residing within said MCN, wherein each OCS is included in an ACS of a process which created it;

permitting access to said object in response to detecting:

said request is from a first user; and

a UCS of the first user is a superset of an OCS of said object;

denying access to said object in response to detecting:

said request is from the first user; and

a UCS of the first user is not a superset of an OCS of said object;

permitting access to said object in response to detecting:

said request is from a process; and

an ACS of said process is a superset of an OCS of said object; and

denying access to said object in response to detecting:

said request is from said process; and

an ACS of said process is not a superset of an OCS of said object;

wherein a given OCS comprises a first set of communities, a given UCS is a superset of the given OCS if at least all of the first set of communities are also included in the given UCS, and a given ACS is a superset of the given OCS if at least all of the first set of communities are also included in the given ACS.

2. The method of claim 1, wherein said object is an operating system controlled resource.

3. The method of claim 2, wherein said object is selected from the group consisting of a file system, a storage volume, a directory, a file, a record, a memory region, a queue, a pipe, a socket, a port, or an input/output device.

4. The method of claim 1, wherein an initial owner of said object is a creator of said object.

5. The method of claim 1, further comprising permitting an owner of said object to designate a first user as a new owner of said object, in response to detecting a UCS of said first user is a superset of said OCS.

6. The method of claim 1, further comprising allowing a first process to change said OCS of said object to a subset of said ACS of said first process, in response to detecting an owner of said first process is an owner of said object and said ACS is a superset of said OCS.

7. (Canceled).

8. (Canceled).

9. The method of claim 1, wherein said CIB further includes a creator and a current

owner for each object residing within said MCN.

10. A Multi-Community Node (MCN) comprising:

a community information base (CIB), wherein said CIB includes:

a user community set (UCS) for each user of said MCN, wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community;

an application community set (ACS) for each application on said MCN, wherein for a given application and associated ACS, a given community is a member of the ACS if the given application runs on behalf of a user in the given community; and

an object community set (OCS) for each object residing within said MCN, wherein each OCS is included in an ACS of a process which created it;

a processing unit configured to:

receive a request for access to an object;

consult said CIB responsive to said request;

permit access to said object in response to detecting:

said request is from a first user; and

a UCS of the first user is a superset of an object community set (OCS) of said object;

deny access to said object in response to detecting:

said request is from the first user; and

a UCS of the first user is not a superset of an OCS of said object;

permit access to said object in response to detecting:

said request is from a process; and

an ACS of said process is a superset of said OCS; and

deny access to said object in response to detecting:

said request is from said process; and

an ACS of said process is not a superset of an OCS of said object;

wherein a given OCS comprises a first set of communities, a given UCS is a superset of the given OCS if at least all of the first set of communities are also included in the given UCS, and a given ACS is a superset of the given OCS if at least all of the first set of communities are also included in the given ACS.

11. The MCN of claim 10, wherein said object is an operating system controlled resource.

12. The MCN of claim 11, wherein said object is selected from the group consisting of a file system, a storage volume, a directory, a file, a record, a memory region, a queue, a pipe, a socket, a port, or an input/output device.

13. The MCN of claim 10, wherein an initial owner of said object is a creator of said object.

14. The MCN of claim 10, wherein said processing unit is further configured to permit an owner of said object to designate a first user as a new owner of said object, in response to detecting a UCS of said first user is a superset of said OCS.

15. The MCN of claim 10, wherein said processing unit is further configured to allow a first process to change said OCS of said object to a subset of said ACS of said first process, in response to detecting an owner of said first process is an owner of said object and said ACS is a superset of said OCS.

16. (Canceled).

17. The MCN of claim 10, wherein said CIB further includes a creator and a current owner for each object residing within said MCN.

18. A computer system comprising:

a computer network; and

a multi-community node (MCN) coupled to said computer network, wherein said MCN comprises:

a community information base (CIB), wherein said CIB includes:

a user community set (UCS) for each user of said MCN, wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community;

an application community set (ACS) for each application on said MCN, wherein for a given application and associated ACS, a given community is a member of the ACS if the given application runs on behalf of a user in the given community; and

an object community set (OCS) for each object residing within said MCN, wherein each OCS is included in an ACS of a process which created it;

a processing unit configured to:

receive a request for access to an object;

consult said CIB responsive to said request;

permit access to said object in response to detecting:

said request is from a first user; and

a UCS of the first user is a superset of an object community set (OCS) of said object;

deny access to said object in response to detecting:

said request is from the first user; and

a UCS of the first user is not a superset of an OCS of said object;

permit access to said object in response to detecting:

said request is from a process; and

an ACS of said process is a superset of said OCS; and

deny access to said object in response to detecting:

said request is from said process; and

an ACS of said process is not a superset of an OCS of said object;

wherein a given OCS comprises a first set of communities, a given UCS is a superset of the given OCS if at least all of the first set of communities are also included in the given UCS, and a given ACS is a superset of the given OCS if at least all of the first set of communities are also included in the given ACS.

19. The computer system of claim 18, wherein said object is an operating system controlled resource.

20. The computer system of claim 19, wherein said object is selected from the group consisting of a file system, a storage volume, a directory, a file, a record, a memory region, a queue, a pipe, a socket, a port, or an input/output device.

21. The computer system of claim 18, wherein an initial owner of said object is a creator of said object.

22. The computer system of claim 18, wherein said processing unit is further configured to permit an owner of said object to designate a first user as a new owner of said object, in response to detecting a UCS of said first user is a superset of said OCS.

23. The computer system of claim 18, wherein said processing unit is further configured to allow a first process to change said OCS of said object to a subset of said ACS of

said first process, in response to detecting an owner of said first process is an owner of said object and said ACS is a superset of said OCS.

24. (Canceled).

25. The computer system of claim 18, wherein said CIB further includes a creator and a current owner for each object residing within said MCN.

26. A carrier medium comprising program instructions, wherein said program instructions are executable to:

receive a request for access to an object;

consult a community information base (CIB) responsive to said request, wherein said CIB includes:

a user community set (UCS) for each user of said MCN, wherein for a given user and associated UCS, a given community is a member of the UCS if the given user is a member of the given community;

an application community set (ACS) for each application on said MCN, wherein for a given application and associated ACS, a given community is a member of the ACS if the given application runs on behalf of a user in the given community; and

an object community set (OCS) for each object residing within said MCN, wherein each OCS is included in an ACS of a process which created it;

permit access to said object in response to detecting:

said request is from a first user; and

a UCS of the first user is a superset of an OCS of said object; and

deny access to said object in response to detecting:

said request is from the first user; and

a UCS of the first user is not a superset of an OCS of said object;

permit access to said object in response to detecting:

said request is from a process; and

an ACS of said process is a superset of an OCS of said object; and

deny access to said object in response to detecting:

said request is from said process; and

an ACS of said process is not a superset of an OCS of said object;

wherein a given OCS comprises a first set of communities, a given UCS is a superset of the given OCS if at least all of the first set of communities are also included in the given UCS, and a given ACS is a superset of the given OCS if at least all of the first set of communities are also included in the given ACS.

27. The carrier medium of claim 26, wherein said object is an operating system controlled resource.

28. The carrier medium of claim 27, wherein said object is selected from the group consisting of a file system, a storage volume, a directory, a file, a record, a memory region, a queue, a pipe, a socket, a port, or an input/output device.

29. The carrier medium of claim 26, wherein an initial owner of said object is a creator of said object.

30. The carrier medium of claim 26, wherein said program instructions are further executable to permit an owner of said object to designate a first user as a new owner of said object, in response to detecting a UCS of said first user is a superset of said OCS.

31. The carrier medium of claim 26, wherein said program instructions are further executable to allow a first process to change said OCS of said object to a subset of said ACS of said first process, in response to detecting an owner of said first process is an owner of said object and said ACS is a superset of said OCS.

32. (Canceled).

33. (Canceled).

34. The carrier medium of claim 26, wherein said CIB further includes a creator and a current owner for each object residing within said MCN.

IX. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131 or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

X. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.